Cryptanalysis of an anonymous wireless authentication and conference key distribution scheme

Qiang Tang and Chris J. Mitchell
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
{qiang.tang, c.mitchell}@rhul.ac.uk

19th February 2005

Abstract

In this paper we analyse an anonymous wireless authentication and conference key distribution scheme which is also designed to provide mobile participants with user identification privacy during the conference call. The proposed scheme consists of three sub-protocols: the Call Set-Up Authentication Protocol, the Hand-Off Authentication Protocol, and the Anonymous Conference Call Protocol. We show that the proposed scheme suffers from a number of security vulnerabilities.

1 Introduction

In [1], Wang proposed an anonymous wireless authentication and conference key distribution scheme, which enables authentication between mobile users and base stations (also between mobile users and the mobile switching center (MSC)) and secure conference key distribution in the mobile system. The proposed scheme is claimed to possess the following advantages:

1. It provides the mobile user with user identification privacy which can prevent outsiders from tracing the location of a mobile.
2. It provides anonymity for the mobile users in the conference call so that one participant in the conference does not know who else has joined the conference call.

Wang [1] claimed that the proposed scheme is secure and achieves all the intended properties; however our analysis demonstrates that a number of security vulnerabilities exist in the proposed protocols: (1) In the Call Set-Up Authentication Protocol a malicious base station can cheat the mobile user; (2) In the Hand-Off Authentication Protocol a malicious base station can impersonate a valid base station; (3) In the Anonymous Conference Call Protocol a participant can determine whether or not another mobile user has taken part in the conference call, so that the anonymity property is undermined.

The remainder of this paper is organised as follows. In Section 2, we review the proposed authentication and key distribution scheme. In Section 3, we describe vulnerabilities in the proposed protocols. In Section 4, we conclude the paper.

2 Review of the proposed scheme

In the proposed scheme three kinds of entity are involved in the protocols, namely the MSC, the base stations, and the mobile users. The scheme is designed for use by the subscribers of the same MSC. The MSC has a number of service domains, each uniquely enabled by a base station. The mobile user communicates with the base station via a radio link, in which we suppose the data is transferred in plain-text and an eavesdropper can intercept the message. The base station communicates with the MSC via a wire-line link, which is assumed to be a channel secure against both passive and active adversaries. The mobile user cannot communicate with the MSC directly; communications between them must be forwarded by a base station.

The proposed scheme consists of the following three sub-protocols:

1. Call Set-Up Authentication Protocol: This protocol is used to achieve mutual authentication between the user and the MSC. It also enables authentication between the mobile user and the base station.
2. Hand-Off Authentication Protocol: This protocol is used for re-authentication when the user moves to a new service domain during a session.
3. Anonymous Conference Call Protocol: This protocol is used for the anonymous establishment of a conference key among the participating users.

The three protocols apply to a closed group of at most $m + 1$ members for some m, the members of which are written MU_0, MU_1, $\cdots$. The size of m is constrained by the size of other system parameters, notably the length of

the prime p (as described below). The Call Set-up Authentication Protocol describes how mobile user MU_i joins such a group. User MU_0 is a 'special' member, responsible for initiating every conference call. In an initialisation phase (prior to executing any of the protocols making up the scheme), the MSC chooses a large prime number p, and an integer l with a bit length of at least 250.

Then the MSC sets $n = m+l$ and computes two vectors: $A = (a_1, a_2, \cdots, a_n)$ and $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_n)$, which satisfy:

$$p > \sum_{j=1}^{n} (a_j \lambda_j \mod p)$$

and

$$a_i \lambda_i > \sum_{1 \le j \le n, j \ne i} (a_j \lambda_j \mod p)$$

for any i, $1 \le i \le n$. The MSC computes $y_i = \lambda_i a_i \mod p$ and sets (λ_i, y_i) to be the secret keys for MU_i. The vector A and the prime p are the public keys, where a_i is the public key of MU_i. MU_i keeps (λ_i, y_i) secret inside the handset. In the initialisation phase, when mobile user MU_i registers at the MSC, the MSC and MU_i agree and store a random check number $RC_{i,0}$ (the second subscript indicates the number of protocol rounds completed by MU_i since registration). The MSC chooses an RSA key pair, publishes the public key $e = 3$ and the modulus n, and keeps the private key d secret. A collision-resistant hash function h is agreed by all the entities.

In the following description, $||$ represents concatenation, $E_k(m)$ represents encrypting m with secret key k using a symmetric encryption algorithm, $\oplus$ represents the bit-wise exclusive or operation, and $\mathrm{ID_X}$ represents the identity of entity X.

2.1 Call Set-Up Authentication Protocol

This protocol is initiated by a mobile user during conference call establishment. Without loss of generality, we suppose this is the $(v+1)$-th $(v \ge 0)$ round of the protocol for MU_i.

1. MU_i selects a nonce K_{s_i}, encrypts $(\mathrm{ID_{MU_i}}||RC_{i,v}||K_{s_i})$ using the public key of the MSC: i.e. $AU_{\mathrm{MU}_i} = (\mathrm{ID_{MU_i}}||RC_{i,v}||K_{s_i})^3 \mod n$, and then sends AU_{MU_i} to the Base Station BS for the service domain where MU_i is located. K_{s_i} will be used as the secret key between MU_i and the MSC during the conference call.

2. After receiving AU_{MU_i}, BS forwards AU_{MU_i} and its identity $\mathrm{ID_{BS}}$ to the MSC.

3. When the MSC receives AU_{MU_i} and $\mathrm{ID}_{\mathrm{BS}}$, it decrypts AU_{MU_i} to obtain $(\mathrm{ID}_{\mathrm{MU}_i}||RC_{i,v}||K_{s_i})$. Then the MSC checks whether $\mathrm{ID}_{\mathrm{MU}_i}$ is in its database and that the received $RC_{i,v}$ is equal to the value stored in its database. If both checks succeed, the MSC accepts MU_i as a legal subscriber; otherwise, the MSC terminates the protocol.

   The MSC selects a new random check number $RC_{i,v+1}$ for MU_i to use in the next run of this protocol. Then the MSC computes $NR = RC_{i,v} \oplus RC_{i,v+1}$ and generates a secret key $S_{\mathrm{BS}} = (h(\mathrm{ID}_{\mathrm{BS}}||RC_{i,v}) \cdot RC_{i,v})^d \bmod n$. Then the MSC sends $\{S_{\mathrm{BS}}, NR\}$ to BS.

4. After receiving the message, BS chooses a random number r and computes:
$$X_{\mathrm{BS}} = g^{-3r} \bmod n, \text{ and } Y_{\mathrm{BS}} = S_{\mathrm{BS}} \cdot g^r \bmod n$$
   Then BS sends $\{\mathrm{ID}_{\mathrm{BS}}, X_{\mathrm{BS}}, Y_{\mathrm{BS}}, NR\}$ to MU_i.

5. After receiving $\{\mathrm{ID}_{\mathrm{BS}}, X_{\mathrm{BS}}, Y_{\mathrm{BS}}, NR\}$ from BS, MU_i verifies:
$$\frac{(Y_{\mathrm{BS}})^3 X_{\mathrm{BS}}}{RC_{i,v}} \bmod n = h(\mathrm{ID}_{\mathrm{BS}}||RC_{i,v}) \bmod n$$
   If the verification succeeds, MU_i regards BS as a valid base station; otherwise, MU_i terminates the protocol.

   MU_i computes $RC_{i,v+1} = NR \oplus RC_{i,v}$ and replaces $RC_{i,v}$ with $RC_{i,v+1}$. MU_i also computes and stores $V_{\mathrm{BS}} = h(\mathrm{ID}_{\mathrm{BS}}||RC_{i,v})$ for future use when a hand-off occurs.

6. MU_i sends an acknowledgment to BS, and BS forwards the acknowledgment to the MSC.

7. After receiving the acknowledgment from MU_i, the MSC replaces $RC_{i,v}$ in the database with $RC_{i,v+1}$ and stores S_{BS} for later use in hand-off.

2.2 Hand-Off Authentication Protocol

During an established conference call (suppose it is the $(v+1)$-th $(v \geq 0)$ conference call for MU_i), MU_i might move from the service domain of BS to the service domain of a different Base Station BS′. In this case, the following hand-off protocol is required for a new mutual authentication between MU_i and BS′.

1. BS generates a nonce n_B and sends it to both MU_i and the MSC.

2. The MSC determines (by some means) the new base station, say BS′, for MU_i, and computes $S_{\mathrm{BS}'} = (h(\mathrm{ID}_{\mathrm{BS}'}))^d S_{\mathrm{BS}} \bmod n$. The MSC then computes and sends $E_{K_{s_i}}(n_B)$ and $S_{\mathrm{BS}'}$ to BS′.

3. MU_i sends $E_{K_{s_i}}(n_B)$ to BS'. Here we assume that the routing mechanism used in the network enables MU_i to determine the identity of its new base station.

4. BS' compares the two values of $E_{K_{s_i}}(n_B)$ received from MU_i and the MSC. If they match, BS' regards MU_i as a valid subscriber; otherwise, BS' terminates the protocol.

5. After receiving $S_{\mathrm{BS}'}$, BS' further chooses a random number r', and computes:
$$X_{\mathrm{BS}'} = g^{-3r'} \bmod n$$
$$Y_{\mathrm{BS}'} = S_{\mathrm{BS}'} \cdot g^{r'} \bmod n$$
Then BS' sends $\{\mathrm{ID}_{\mathrm{BS}'}, X_{\mathrm{BS}'}, Y_{\mathrm{BS}'}\}$ to MU_i.

6. After receiving $\{\mathrm{ID}_{\mathrm{BS}'}, X_{\mathrm{BS}'}, Y_{\mathrm{BS}'}\}$ from BS', MU_i verifies:
$$\frac{(Y_{\mathrm{BS}'})^3 X_{\mathrm{BS}'}}{RC_{i,v}} \bmod n = V_{\mathrm{BS}} \cdot h(\mathrm{ID}_{\mathrm{BS}'}) \bmod n$$
If the verification succeeds, MU_i regards BS' as a valid base station.

After the successful protocol execution, MU_i stores $V_{\mathrm{BS}'} = V_{\mathrm{BS}} \cdot h(\mathrm{ID}_{\mathrm{BS}'})$ for future authentication. The MSC stores $S_{\mathrm{BS}'}$ for future use.

2.3 Anonymous Conference Call Protocol

Suppose some set of k ($k < m$) users wish to establish a conference key. Without loss of generality, suppose the users are MU_1, MU_2, $\cdots$, MU_k. They perform the following protocol.

1. MU_0 issues a participation list for the conference call, and constructs the binary vector $R = (r_1, \cdots, r_m)$, where $r_i = 1$ if and only if MU_i is to be a member of the conference, i.e. in this case $r_1 = \cdots = r_k = 1$ and $r_{k+1} = \cdots = r_m = 0$. MU_0 chooses a vector $(w_1, \cdots, w_l)$, each element of which is randomly chosen from $\{0, 1\}$. MU_0 computes:
$$Z = \sum_{i=1}^{m} a_i r_i + \sum_{i=1}^{l} a_{m+i} w_i$$
and puts
$$AU_{\mathrm{MU}_0} = (\mathrm{ID}_{\mathrm{MU}_0} || \mathrm{ID}_{\mathrm{MU}_1} || \cdots || \mathrm{ID}_{\mathrm{MU}_k} || RC_{i,v} || K_{s_0})^3 \bmod n$$
Then MU_0 sends $\{Z, AU_{\mathrm{MU}_0}\}$ to the MSC via a base station.

2. MU_0 and MSC authenticate each other using the Call Set-Up Authentication Protocol. If the protocol is successfully completed, the MSC broadcasts Z to all the mobile users in the same group. The MSC decrypts AU_{MU_0} to obtain the identities of the users participating in the conference.

3. When MU_i $(1 \leq i \leq m)$ receives the broadcast message, it can compute $R_i' = \lambda_i Z \bmod p$, where λ_i is the private key of MU_i. If $R_i' < y_i$, then MU_i can deduce that $r = 0$ and hence MU_i is excluded from this call; otherwise, we must have $r = 1$ and hence MU_i is included in this conference call.

   As a result, the users $\mathrm{MU}_1, \mathrm{MU}_2, \cdots, \mathrm{MU}_k$ will know that they are included in the conference call. Each MU_j $(1 \leq j \leq k)$ computes $(\mathrm{ID}_{\mathrm{MU}_j} || RC_{j,w} || K_{s_j})^3 \bmod n$ and sends it to the MSC (for the simplicity of our description, we assume that this is the $(w+1)$-th $(w \geq 0)$ round of the protocol for MU_j). Notice that this is the first message of the Call Set-Up Authentication Protocol between MU_j and the MSC.

4. After receiving $(\mathrm{ID}_{\mathrm{MU}_j} || RC_{j,w} || K_{s_j})^3 \bmod n$, the MSC decrypts it to obtain $\mathrm{ID}_{\mathrm{MU}_j}$, $RC_{j,w}$, and K_{s_j}. Then the MSC checks whether the identity $\mathrm{ID}_{\mathrm{MU}_j}$ is identical to one of the identities he stored in Step 2. If the check fails, the user is rejected. Once MU_j is accepted, MU_j and the MSC proceed through the rest of the Call Set-Up Authentication Protocol. If the protocol is successfully completed, $\mathrm{ID}_{\mathrm{MU}_j}$ and the MSC will share a common secret key K_{s_j}.

5. After finishing the mutual authentication process with all the participants, the MSC uses the coordinate points $(\mathrm{ID}_{\mathrm{MU}_0}, K_{s_0})$ and $(\mathrm{ID}_{\mathrm{MU}_j}, K_{s_j})$ $(1 \leq j \leq k)$ to construct a Lagrange interpolating polynomial $f(z)$ of degree k over $GF(p)$. The MSC computes $K_c = f(0)$ as the common session key for the conference. Then the MSC selects k distinct coordinate points (a_t, b_t), $t = 1, 2, \cdots, k$ from the polynomial $f(z)$ and broadcasts them to the participating users.

6. On receiving (a_t, b_t), $t = 1, 2, \cdots, k$, MU_j $(1 \leq j \leq k)$ reconstructs the interpolating polynomial $f(z)$ using (a_t, b_t), $t = 1, 2, \cdots, k$ and his own coordinate pair $(\mathrm{ID}_{\mathrm{MU}_j}, K_{s_j})$, and then computes $K_c = f(0)$. MU_0 can computes K_c in the same way.

3 Security Vulnerabilities

Wang (see, for example, [1]) claimed that the proposed scheme is secure and achieves all the intended properties; however we show that the protocols suffer from a number of vulnerabilities. It should be noted that our analysis

has been carried out theoretically, and we do not provide implementation details of the attacks.

- First observe that the Call Set-Up Authentication Protocol involves encrypting a data string by simply applying the RSA primitive (i.e. modular exponentiation), without any preliminary padding or masking. This has, for a number of years, been deemed very bad practice for a variety of reasons. It is generally accepted that use of the RSA primitive for encryption requires that data be first masked and padded by some means, e.g. OAEP [2].

- Since the acknowledgement sent by the mobile user to the base station in the Call Set-Up Authentication Protocol is not authenticated, an attacker can easily mount a denial of service attack. To deploy an attack, the attacker just needs to substitute the value NR with NR' ($NR' \neq NR$) in step 5 of the protocol. As a result MU_i will then lose synchronism with the MSC, and all subsequent instances of the Call Set-Up Authentication Protocol for MU_i will fail.

- In some circumstances it is possible for a malicious base station to impersonate the MSC to cheat the mobile user in the Call Set-Up Authentication Protocol. For simplicity, we show the attack assuming that MU_i executes the protocol on two consecutive occasions via the same base station BS.

  In the Call Set-Up Authentication Protocol the value NR is transferred in plain-text, and so BS can record the value of NR used in every round of the protocol. Because there is no authentication for the nonce NR transported in step 4 of the protocol, then in the $(v+2)$-th ($v \geq 0$) round of the protocol BS can replace NR with $RC_{i,v} \oplus RC_{i,v+1}$, which equals the NR used in the previous round. The protocol will successfully end, and MU_i will store the check number as $RC_{i,v+2} = RC_{i,v+1} \oplus RC_{i,v} \oplus RC_{i,v+1} = RC_{i,v}$. In the $(v+3)$-th round of the protocol BS can impersonate the MSC to MU_i as follows.

  1. MU_i selects a nonce K_{s_i}, then computes and sends:

     $$AU_{\mathrm{MU}_i} = (\mathrm{ID}_{\mathrm{MU}_i} || RC_{i,v+2} || K_{s_i})^3 \bmod n$$

     to BS. K_{s_i} will be used as the secret key between MU_i and the MSC.

  2. After receiving AU_{MU_i}, BS sets the value of NR to be a random number and puts $S_{\mathrm{BS}} = (h(\mathrm{ID}_{\mathrm{BS}} || RC_{i,v}) \cdot RC_{i,v})^d \bmod n$, which is the same as the value used the $(v+1)$-th round of the Call Set-Up

Authentication Protocol. Then BS chooses a random number r and computes:

$$X_{\mathrm{BS}} = g^{-3r} \bmod n$$

$$Y_{\mathrm{BS}} = S_{\mathrm{BS}} \cdot g^{r} \bmod n$$

Then BS sends $\{\mathrm{ID}_{\mathrm{BS}}, X_{\mathrm{BS}}, Y_{\mathrm{BS}}, NR\}$ to MU_i.

3. After receiving $\{\mathrm{ID}_{\mathrm{BS}}, X_{\mathrm{BS}}, Y_{\mathrm{BS}}, NR\}$ from BS, MU_i verifies:

$$\frac{(Y_{\mathrm{BS}})^3 X_{\mathrm{BS}}}{RC_{i,v+2}} \bmod n = h(\mathrm{ID}_{\mathrm{BS}} || RC_{i,v+2})$$

Since $RC_{i,v+2} = RC_{i,v}$, the verification will succeed and the impersonation attack is successfully completed.

It should be noted that any malicious party equipped with the means to emulate a base station and intercept traffic sent and received by a mobile user could launch this attack by impersonating BS.

- Suppose, during the conference call, MU_i transfers from the service domain of BS to the service domain of BS$'$. Then any attacker equipped with the means to emulate a base station, who has intercepted the hand-off authentication history over the radio link, can deploy an impersonation attack on the next occasion that MU_i transfers to a domain serviced by another base station BS$''$.

  Suppose the intercepted history data of MU_i is $\{\mathrm{ID}_{\mathrm{BS}'}, X_{\mathrm{BS}'}, Y_{\mathrm{BS}'}\}$ in step 5 of the Hand-Off Authentication Protocol. Then the attacker can impersonate BS$''$ to execute the Hand-Off Authentication Protocol as follows.

  1. The attacker generates a nonce n_B and sends it to MU_i.
  2. MU_i sends $E_{K_{s_i}}(n_B)$ to the attacker.
  3. The attacker uses $\{\mathrm{ID}_{\mathrm{BS}'}, X_{\mathrm{BS}'}, Y_{\mathrm{BS}'}\}$ to compute:

$$Y_{\mathrm{BS}''} = Y_{\mathrm{BS}'} = S_{\mathrm{BS}} \cdot g^{r'} \bmod n$$

$$X_{\mathrm{BS}''} = h(\mathrm{ID}_{\mathrm{BS}''}) \cdot X_{\mathrm{BS}'} = h(\mathrm{ID}_{\mathrm{BS}''}) \cdot g^{-3r'} \bmod n$$

  The attacker then sends $\{\mathrm{ID}_{\mathrm{BS}''}, X_{\mathrm{BS}''}, Y_{\mathrm{BS}''}\}$ to MU_i.

  4. After receiving $\{\mathrm{ID}_{\mathrm{BS}''}, X_{\mathrm{BS}''}, Y_{\mathrm{BS}''}\}$ from the attacker, MU_i verifies:

$$\frac{(Y_{\mathrm{BS}''})^3 X_{\mathrm{BS}''}}{RC_{i,v}} \bmod n = V_{\mathrm{BS}'} \cdot h(\mathrm{ID}_{\mathrm{BS}''}) \bmod n$$

  and the impersonation attack succeeds.

- Although the the Anonymous Conference Call Protocol is designed to provide anonymity for the participants, we show that it is possible for a participant, MU_i say, to find out whether another user has taken part in the conference. The attack is based on the assumption that the attacking mobile user knows the identity of the victim user and can track him.

  Suppose MU_i tracks MU_j and intercepts all the messages to and from MU_j. When MU_j transfers from the service domain of BS_1 to the service domain BS_2, if MU_j has taken part in a conference call then MU_i can intercept the n_B and $E_{K_{s_j}}(n_B)$ from the Hand-Off Authentication Protocol of MU_j. Then MU_i computes the secret key $K^*_{s_j}$ between MU_j and the MSC (this is meaningful only if MU_{i_l} has taken part in the conference) using the the interpolating polynomial $f(z)$, which belongs to the conference call that MU_i has taken part in. MU_i then knows that MU_j has taken part in the conference if $E_{K_{s_j}}(n_B) = E_{K^*_{s_j}}(n_B)$.

  Furthermore, if MU_i discovers that MU_j has taken part in the same conference call, then, using K_{s_j}, MU_i can impersonate MU_j when MU_j transfers to another service domain.

4 Conclusion

In this paper we have analysed an anonymous wireless authentication and conference key distribution scheme which is also designed to provide mobile participants with user identification privacy during the conference call. We show that all the proposed protocols suffer from significant security vulnerabilities.

References

[1] S.-J. Wang. Anonymous wireless authentication on a portable cellular mobile system. *IEEE Transactions on Computers*, 53(10):1317–1329, 2004.

[2] A. W. Dent and C. J. Mitchell. *User's Guide to Cryptography and Standards*. Artech House, 2005.